Fino a prova contraria

Giancarlo Capozzoli

17 lug

Roma. L'Infragard-FBI e il Terrorismo-Cyber di Prossima Generazione.

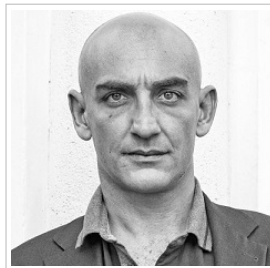
Articolo redatto in collaborazione con l'Ing. Luciano Magaldi (PhD), membro operativo del reparto italo-americano del partneriato federale americano (pubblico-privato) Infragard-Federal Bureau of Investigation (FBI). L'ing. Luciano Magaldi è stato Security Engineer presso Google Irlanda a Dublino, Irlanda, presso Apple European Headquarters a Cork, Irlanda, e Amazon Slovacchia a Bratislava.

Chiunque abbia mai citato erroneamente riconosce l'importanza del contesto. Ipotesi sbagliate su concetti, parole e frasi portano facilmente a malintesi. Nella comunità delle forze dell'ordine federali degli Stati Uniti gli ufficiali che usano un' arma in servizio per difendersi o difendere innocenti dalle reali minacce terroristiche, possono uccidere. Il contesto spesso funge da variabile cruciale che giustifica l'uso della forza mortale. L'omicidio uccide sempre, ma uccidere non è sempre omicidio. Allo stesso modo, una conoscenza accurata dei contesti reali nella lotta al terrorismo internazionale nella vita reale può migliorare la chiarezza e lo svelamento dell'intento oscurante delle nuove minacce cibernetiche, ad opera non dei soliti hacker ma di reali operatori del terrorismo cibernetico. Ed essi hanno lo stesso intento: uccidere il reale attraverso il loro impenetrabile mondo virtuale.

Ma cominciamo con il chiarire cosa è Il terrorismo cibernetico senza usare termini indefiniti e fraintendibili che potrebbero facilmente portare ad una conversazione che proceda lungo linee parallele piuttosto che una traccia intersecante: esso è una componente della guerra occulta, giornaliera, che avviene in infrastrutture elettrodottistiche a livello globale tra agenzie di intelligence ed operatori terroristici esperti di informatica. La guerra mondiale di livello cyber nella presente era dell'informazione ormai consiste in operazioni offensive e difensive contro risorse e infrastrutture critiche di natura "win-lose", in cui spesso si esce vincitori o perdenti, carnefici o vittime. Alcuni ricercatori di alto livello dell' intelligence statunitense la definiscono come "la guerra in cui le operazioni di combattimento si sono spostate da in un ambiente di campo di battaglia reale ad uno ad alta tecnologia, in cui entrambe le parti nemiche in rivalità usano mezzi, attrezzature o sistemi informatici al fine di ottenere, controllare e utilizzare le informazioni critiche dell'altra parte, per evitare conseguenze critiche e/o nefaste ai detrimenti della propria sicurezza nazionale".

Oramai, oggigiorno, i terroristi cibernetici hanno raggiunto alti livelli di sofisticatezza in quanto sfruttano le ultime tecnologie informatiche e le più recenti tecniche di ingegneria sociale, via web, con la piena e accurata comprensione dell'utilizzo della crittografia, sia criptologica sia crittanalitica, entrando nel campo militare della ricognizione radar, della ricognizione aerea ad alta quota, della sorveglianza elettronica, dell'intelligence acquisita elettronicamente, e della steganografia. La distinzione nella strategia che vogliono raggiungere ed implementare non si basa solo, tuttavia, sugli strumenti tecnologici impiegati, ma dipendono anche e soprattutto dal contesto e dall'obiettivo in cui operano, da soli o in gruppi.

A mo' di esemplificazione: nel 1991, in risposta al rifiuto di Saddam Hussain di ritirarsi dal Kuwait, durante l' Operazione "Desert Storm", gli Americani e le Forze della Coalizione usarono tutte le strategie, tecnologie e tecniche allora

CHI SONO

CERCA NEL BLOG

Cerca

ARTICOLI RECENTI

- Roma. L'Infragard-FBI e il Terrorismo-Cyber di Prossima Generazione.
- Roma. Terrorismo, radicalizzazione, psy-ops, sicurezza, intelligence. Una intervista a Sabrina Magris, Presidente di École Universitaire Internationale
- Roma. Un viaggio politico senza mappe. Una intervista all'Ambasciatore Alessandro Minuto Rizzo
- Roma. Future Combat Naval System 2035. Una intervista all'Ammiraglio Enrico Vignola.
- Roma. Evoluzione della società e cultura dell'intelligence. Una intervista al professor Marco Bacini, LUM

COMMENTI RECENTI

- Mr WordPress su Ciao mondo!!

luglio: 2021

L	M	M	G	V	S	D
				2	3	
5	6		8	9	10	
12		14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

ARCHIVI

- luglio 2021
- giugno 2021
- maggio 2021
- aprile 2021
- marzo 2021
- febbraio 2021
- gennaio 2021
- dicembre 2020
- novembre 2020
- ottobre 2020
- settembre 2020
- agosto 2020
- luglio 2020

conosciute per attuare l'inoculazione clandestina di virus e bombe logiche nei computer e nelle periferiche del centro di comando e controllo della "Guardia Repubblicana Irachena", causando l'interruzione e l'alterazione del "targeting" e del lancio dei missili Scud 5: i combattenti militari che si impegnarono a vicenda sul campo di battaglia reale attaccarono le infrastrutture critiche, anche informatiche, in gran parte civili: allora si cominciò a diffondere il termine di terrorismo cibernetico. Ma vediamo in che modo esso confluisce in questo nostro ragionamento.

Il termine deriva da "Cyber-Terror", letteralmente "ciberterrore", coniato negli anni '80 da Barry Collin che aveva già discusso di questa dinamica del terrorismo come trascendenza dal regno fisico a quello virtuale in qualità di intersezione, di convergenza di questi due mondi. L'illustre "Center for Strategic and International Studies (CSIS) degli USA lo ha definito come "l'uso di strumenti di rete informatica per inibire le infrastrutture nazionali critiche, ad esempio l'energia , i trasporti, le operazioni governative, …, o per costringere o intimidire un Governo o una popolazione civile, spesso occidentale". Ma esso può anche essere definito in qualità di "intimidazione" da parte di una impresa civile attraverso l'uso dell'alta tecnologia per realizzare obiettivi politici, religiosi o ideologici, mediante azioni che si traducono nella disabilitazione o nell'eliminazione di dati o informazioni critiche dell' infrastruttura nemica.

Ma facciamo un'altra illustrazione esemplificativa di tipo dimensionale cui mira il terrore cyber: il presente articolo non è paragonabile alle proprietà della Biblioteca del Congresso degli Stati Uniti d'America. La perdita del primo sarebbe traumatica per l'autore, ma avrebbe un impatto modesto su poche altre persone. La perdita invece di una proprietà informatica del Congresso americano, probabilmente insostituibile, si rivelerebbe devastante se un attacco cibernetico avesse cancellato quei files di importanza strategica nazionale. Naturalmente, nessuno dei due poteva paragonarsi alla perdita di una vita umana ma, se i dati o le informazioni provenienti da una qualsiasi base di dati delle infrastrutture critiche della nazione washingtoniana fossero attaccati e distrutti, ciò avrebbe certamente un impatto devastante sulla qualità della vita di numerosi statunitensi.

Un altro esperto di terrorismo cyber americano ha affermato che se le persone si fossero informate sulla spesa annuale investita per la sicurezza nazionale delle informazioni elettroniche, avrebbero dovuto calcolare il doppio di quella stessa stima presentata al Congresso in via preventiva. Recentemente, uno studente laureato ha osservato che "Il terrorismo cyber è una minaccia critica per la sicurezza nazionale e l'ordine pubblico che sta facendo aumentare sempre più il budget da investire derivante dalla tassazione dei cittadini statunitensi. Inoltre, ci troviamo anche in un momento storico critico per l'ordine pubblico vista l'attivazione di fascicoli sanitari digitali per la registrazione elettronica delle vaccinazioni anti-Covid-19, dato che il Governo capitolino dovrà elaborare regolamenti sul trasferimento elettronico dei dati per le informazioni pubbliche, oltre che private, che possono essere identificate e accessibili via Internet. Ma quali sono gli obiettivi più vulnerabili dei terroristi informatici ? Che cosa costituisce il significato degli obiettivi e l'entità della minaccia ? Ci importa qualcosa di come si chiama la minaccia? Il terrorismo cyber costituisce un elemento della criminalità informatica?

Per rispondere a tutte questi interrogativi esploriamo da vicino una breve cronostoria dei crimini computeriali: dall'inizio della rivoluzione informatica degli anni 50-60 negli USA, nemmeno le autorità federali di intelligence più importanti hanno raggiunto un consenso su ciò che costituisce, in pratica, la criminalità informatica. Secondo uno dei pionieri di questo genere, il primo evento di tali abusi avvenne nel 1988: il primo processo ai sensi della legge federale, il "Computer Fraud and Abuse Act", Titolo 18, Sezione 1030, Codice Penale degli Stati Uniti, avvenne ai detrimenti di Robert Tappan Morris Jr., allora studente laureato di informatica, il quale scatenò lo storico "Internet Worm".

Lungo il continuum temporale, è qui che la linea inizia a sfocare tra il crimine informatico "convenzionale" e il terrore cibernetico. Questo genere di attività malevola comprende i celebri "Melissa virus (1999)", il virus "I Love You (2001)", il "Worm Red Code (2002)", il virus "Blaster (2004)" e il worm "Conficker (2008). Questi attacchi differiscono da estorsioni, frodi, furti di dati e varie truffe, tutte certamente dannose. Tuttavia, gli atti di terrorismo cyber predefiniti hanno avuto un impatto negativo sulla società, sulla nazione americana, non solo su un individuo ma in tutti gli elementi del tessuto imprenditoriale e/o delle agenzie governative.

giugno 2020
maggio 2020
aprile 2020
marzo 2020
febbraio 2020
gennaio 2020
dicembre 2019
novembre 2019
ottobre 2019
settembre 2019
giugno 2019
aprile 2019
marzo 2019
febbraio 2019
gennaio 2019
dicembre 2018
novembre 2018
ottobre 2018
giugno 2018
maggio 2018
aprile 2018
marzo 2018
febbraio 2018
gennaio 2018

Le limitazioni dello spazio cibernetico governativo non consentono una contabilità “incidente per incidente “degli episodi di terrorismo cyber: ad esempio, durante il caso di Rajib K. Mitra del 2003 in cui si intraprese un attacco contro un sistema radio di emergenza della polizia federale. Inizialmente, le autorità investigarono sugli assalti informatici di Mitra come una violazione della legge statale del Wisconsin ma, alla fine, li consideravano attacchi all'infrastruttura critica. Il caso fu perseguito ai sensi della legge federale mediante il “Computer Fraud and Abuse Act”. Mitra, un lupo solitario, fu processato e condannato il 12 marzo 2004 e successivamente condannato a 96 mesi di reclusione. Successivamente, il suo ricorso fu respinto. I giudici della Corte d'Appello del Settimo Distretto degli Stati Uniti avevano stabilito il tutto all'unanimità, rimarcando che "è impossibile capire perché una persona sana di mente penserebbe che la pena per aver paralizzato un sistema di comunicazione di emergenza da cui possono dipendere vite umane non dovrebbe essere superiore alla pena per l'hackeraggio di un sito Web in cui viene rilasciato un messaggio offensivo”.

Chiaramente, le forze dell'ordine devono rimanere ben informate su ciò che pensano gli esperti. La maggior parte dei professionisti contemporanei rimane almeno cauta. Tuttavia, se le persone aspettano di avere prove assolute positive, potrebbe essere troppo tardi. Le tendenze informatiche sembrano chiare. Nel corso degli ultimi 13 anni di terrorismo cyber, sia il numero che la frequenza dei casi di “disordine digitale” si sono intensificati e la sofisticazione e la diversità dei tipi di attacchi informatici sono aumentate in maniera vertiginosa.

Uno specialista di alto profilo ha sostenuto che "storie di terroristi che controllano la rete elettrica, o aprono dighe, o prendono il controllo della rete di controllo del traffico aereo e si scontrano con aerei, sono storie di paura sempre più realistiche". Ha poi invocato una prospettiva di rapporto costi-benefici: "Dobbiamo capire i rischi reali. Ecco la domanda critica a cui dobbiamo rispondere: quanto è probabile quel tipo di attacco terroristico e quanto è dannoso ?" Un'altra autorità osserva che "anche le minacce alle infrastrutture critiche nazionali stanno diventando sempre più frequenti", e continua: "Gli attacchi informatici sono una delle più grandi minacce alla pace e alla sicurezza internazionali nel XXI secolo". Dove c'è fumo, il fuoco non è ovviamente molto lontano ? e il futuro? quali innovazioni tecnologiche avranno un impatto sulla capacità di servire e proteggere nel prossimo futuro? per quanto riguarda la diffusione del terrorismo cyber, gli esperti assomiglieranno ai proverbiali ciechi che sentono parti diverse dello stesso elefante ? all'orizzonte e a breve termine, sorgeranno meraviglie tecnologiche di cui si avvarranno i terroristi cibernetici senza scrupoli, proprio come altri hanno fatto prima di loro ? ma dove si troveranno le vulnerabilità e quali strumenti tecnologici si utilizzeranno ?

Collegati a tutti questi interrogativi e sicuramente una delle maggiori preoccupazioni, sono i Sistemi di Controllo di Supervisione e Acquisizione Dati (SCADA). Strettamente correlati sono i Sistemi di Controllo Digitale (DCS) e i Controllori a Logica Programmabile (PLC). I sistemi SCADA sono più diffusi rispetto a tutti i PC e laptop messi insieme. Senza l'intervento umano in loco, essi raccolgono automaticamente e in remoto i dati dai sensori nei dispositivi utilizzati per l'elaborazione di dati industriali. Memorizzano le informazioni in basi di dati per la successiva gestione ed elaborazione del sito centrale.

I sistemi SCADA esistono sin dagli anni '60. All'inizio erano autonomi e pochi erano collegati in rete. Oggi, praticamente tutti sono accessibili tramite Internet. Questo può essere ottimo come misura di riduzione dei costi, ma non dal punto di vista della sicurezza informatica. Silenziosamente e senza clamore, i sistemi SCADA sono proliferati rapidamente, per cominciare, nei settori elettrico, petrolifero e del gas, e quindi allagarsi al trattamento delle acque, della gestione dei rifiuti e delle industrie di controllo del traffico marittimo, aereo, ferroviario e automobilistico. I sistemi SCADA sono stati anche incorporati in "reti telefoniche e cellulari, compresi i servizi di emergenza americani".

Questi piccoli ma “oscuri” calcolatori dall’aspetto dronico non hanno praticamente alcuna sicurezza, firewall, router o software antivirus per proteggersi. Sono diffusi in lungo e in largo soprattutto in tutta la nazione washingtoniana, e anche in alcuni dei luoghi più remoti immaginabili. Un hacker anonimo intervistato per un programma televisivo affermò: “I sistemi SCADA sono un approccio standard ai sistemi di controllo che pervadono tutto, dalla fornitura idrica alle tubazioni dei carburanti. " E continuò addirittura

descrivendo che essi eseguono sistemi operativi che li rendono altamente fallaci, vulnerabili, con tanto di tutorial su Toutube.

Non dimentichiamoci delle bombe a impulsi elettromagnetici (EMP) e le armi a radiofrequenza ad alta energia (HERF) che differiscono dai codici maligni, dai virus informatici e dai worm del passato. Mentre questi ultimi rimangono preoccupanti, gli EMP ed HERF costituiscono dei seri pericoli della presente era tecnologica, ma a breve termine. I dispositivi EMP sono compatti e gli autori possono usarli per sovraccaricare i circuiti del computer. Questi dispositivi possono distruggere la scheda madre di un computer e cancellare in modo permanente e irreparabile i dati nei dispositivi di archiviazione di memoria. Come gli EMP, i dispositivi HERF utilizzano radiazioni elettromagnetiche. Anch'essi forniscono calore, energia meccanica o elettrica a un bersaglio. La differenza è che gli individui possono focalizzare i dispositivi HERF su un bersaglio specifico utilizzando un riflettore parabolico. L'HERF, come affermato, non causa danni permanenti, mentre l'EMP lo fà.

Un altro esperto di sicurezza cibernetica ci ha ricordato anche la futura minaccia che grava anche sugli “agenti Internettiani”, ovvero i bot (robot), i web crawler, i web spider e i web scutter, con tutta la famiglia di software che attraversano e indicizzano l’Internet civilmente visibile: essi infatti svolgono attività ripetitive, come il recupero di pagine collegate, parole o frasi specificate o indirizzi di posta elettronica. Sebbene i bot abbiano svolto funzioni benigne, ad esempio la raccolta di indirizzi di posta elettronica, per molti anni, ora si profilano come un problema di sicurezza legato anche alle forze dell’ordine nel futuro a breve termine. Ricerche più recenti supportano questa tesi. Alla luce di queste previsioni, la domanda non è cosa potrebbe accadere domani ma, piuttosto, quanto saranno preparate le forze dell'ordine a proteggere e servire le nazioni più vulnerabili a livello globale.

Le agenzie federali degli USA, responsabili delle indagini sul terrorismo a livello euratlantico e globale, incluso il terrorismo informatico, devono rimanere vigili. Ciò include la garanzia di finanziamenti adeguati per il personale, le attrezzature e la formazione. Ma, oltre a ciò, le forze dell'ordine, soprattutto locali, devono incoraggiare i cittadini a prestare attenzione e a segnalare comportamenti sospetti. Un modello che potremmo importare anche in Europa e in Italia è quello delle forze dell'ordine locali che interagiscono con la comunità del posto, come le accademie di polizia dei cittadini. Questi programmi di crescita sociopolitica possono educare i volontari sulle attività nel regno fisico che dovrebbero essere segnalate. Tuttavia, che dire della trascendenza nel regno virtuale ? Potremmo prendere come esempio un modello che dal 1996 ha cominciato ad operare molto bene: il programma di partenariato di scambio di informazioni di intelligence “InfraGard (da INFRAstructure GARDian, ndr)”, dell’ FBI, ovvero uno sforzo pubblico-privato di condivisione e analisi delle informazioni che si è concentrato sulla raccolta dei talenti dei membri della Comunità Americana per la Sicurezza delle Informazioni (INFOSEC). Essa è una mera conseguenza di ciò che si sente spesso nelle vie e strade statunitensi: "... le forze dell'ordine dovrebbero essere preparate ad affrontare le conseguenze di attacchi informatici difficili da prevedere, ma non ricorrenti, alle infrastrutture critiche della nazione". E ancora: "Vedi qualcosa, denuncia quel qualcosa"; è uno slogan formidabile per la prevenzione del crimine promosso a partire da New York City.

Ciò sembra essere risuonato di recente anche a Times Square, quando un uomo molto vigile, un venditore ambulante, ex-veterano della guerra in Vietnam, avvisò il dipartimento di polizia di New York di un veicolo SUV utilizzato per un tentativo, fortunatamente fallito, di autobomba con tanto di sponsorizzazione talebana. Qualsiasi programma di questo tipo dovrebbe essere potenziato per fornire ai partecipanti esempi di comportamento nella comunità imprenditoriale, compresi quelli in un ambiente di lavoro, che potrebbero allertare autorità a precursori di potenziali crimini informatici. Proprio come qualcuno non ha bisogno di un'istruzione specializzata per riconoscere le minacce nella vita reale, chiunque può riconoscere potrà imparare a riconoscere anche quelle digitali.

Un'autorità Usa ha osservato che "un esempio di comportamento sospetto potrebbe essere un programma dannoso che tenta di installarsi aprendo un documento di Office". Per ridurre la minaccia, i dipendenti potrebbero aggiungere un livello “behaviourale" ai prodotti antivirus". Naturalmente, questo suggerimento potrebbe innervosire molte organizzazioni di controllo delle libertà civili; non vi è alcun motivo per non includere tali agenzie nella discussione, pianificazione e implementazione dell'aspetto appena proposto. Qual è, allora, la linea di fondo in tutto questo ?

Terremoti, uragani, tsunami, tornado, vulcani, fuoriuscite di sostanze tossiche, incendi boschivi e attacchi di squali non si verificano mai con grande frequenza. Tuttavia, esistono precauzioni per proteggere le persone dalle minacce fisiche poste quando si verificano questi eventi violenti naturali ma rari. Sebbene non possano essere previsti con grande precisione, siamo preparati a queste calamità naturali. Allo stesso modo, le forze dell'ordine dovrebbero essere preparate ad affrontare le conseguenze di attacchi informatici difficili da prevedere, ma non ricorrenti, alle infrastrutture critiche della nazione.

I criminali stanno minacciando le nostre dorsali informatiche euroatlantiche, preparandosi a lanciare un attacco su larga scala. Ciò che è chiaro è che accadrà. Ciò che non è ovvio è da chi o quando. Rispettare i consigli di autorità illustri in tale campo quali l'INFOSEC ha portato solo a risultati positivi: un caso convincente ci fu quando una serie di attacchi informatici furono sventati agli inizi degli anni 2010 attraverso percorsi diversi da quelli tradizionali, in cui Al Qaeda aveva già dimostrato di comprendere tali tecniche. Altri paesi, come India, Arabia Saudita, Cina, Francia, Brasile e Spagna, hanno già subito tali attacchi. Inoltre, note multinazionali e corporation statunitensi ed europee hanno già segnalato gravi violazioni mirate ai loro inestimabili codici sorgente e infrastrutture critiche. Ogni giorno i terroristi informatici stanno già eseguendo il ping delle porte e sondando le nostre infrastrutture digitali mentre si sforzano di identificare le eventuali vulnerabilità. Ogni giorno cracker e terroristi si nascondono, attaccano i firewall e imparano di più ogni volta che lo fanno. Oggi come non mai prima, sono necessari adeguate mosse preventive per contrastare tali attacchi.

Le abilità, gli strumenti e le tecniche sono le stesse, ma la guerra dell'era cibernetica è condotta principalmente da attori militari, anche se il terrorismo cyber prende di mira soprattutto i civili. I terroristi informatici attaccheranno indiscriminatamente le infrastrutture critiche della nazione e i civili innocenti. Pertanto, il contesto e gli obiettivi, non gli strumenti tecnologici o la frequenza degli attacchi, sono i delimitatori più appropriati che distingueranno il terrorismo cyber di prossima generazione. Alcuni di questi criminali vengono catturati e perseguiti, ma altri rimangono inosservati e al riparo da occhi indiscreti in qualità di lupi solitari. Per servire al meglio il motto euratlantico delle agenzie di intelligence, "Proteggere e servire", le forze dell'ordine dovranno sempre più prendere a cuore in modo proattivo la sicurezza nazionale di tutta l'area euratlantica, su ogni fronte, arruolando anche i militari e civili più talentuosi.

Condividi:

17 luglio 2021 Senza categoria 0

NESSUN COMMENTO

LASCIA UN COMMENTO

Devi essere registrato per postare un commento.

© 1999-2021 GEDI Gruppo Editoriale S.p.A. - Partita IVA 0090681006 - Pubblicità - Servizio clienti - Chi siamo